# UNITED STATES PATENT AND TRADEMARK OFFICE

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/809,607 | 03/24/2004 | Pawel Oskar Matusz | 1020.P18644 | 7219 |

| | | | |
|---|---|---|---|
| 57035 7590 01/22/2008 | | EXAMINER | |
| KACVINSKY LLC | | LAFORGIA, CHRISTIAN A | |
| C/O INTELLEVATE | | | |
| P.O. BOX 52050 | | ART UNIT | PAPER NUMBER |
| MINNEAPOLIS, MN 55402 | | 2131 | |

| MAIL DATE | DELIVERY MODE |
|---|---|
| 01/22/2008 | PAPER |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1) ☒ Responsive to communication(s) filed on *21 December 2007*.
2a) ☐ This action is **FINAL**.      2b) ☒ This action is non-final.
3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4) ☒ Claim(s) *1-20* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) ☐ Claim(s) _____ is/are allowed.

6) ☒ Claim(s) *1-20* is/are rejected.

7) ☐ Claim(s) _____ is/are objected to.

8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9) ☐ The specification is objected to by the Examiner.

10) ☒ The drawing(s) filed on *24 March 2004* is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a) ☐ All   b) ☐ Some * c) ☐ None of:

    1. ☐ Certified copies of the priority documents have been received.

    2. ☐ Certified copies of the priority documents have been received in Application No. _____.

    3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

## DETAILED ACTION

### Continued Examination Under 37 CFR 1.114

1.      A request for continued examination under 37 CFR 1.114, including the fee set forth in

37 CFR 1.17(e), was filed in this application after final rejection. Since this application is

eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e)

has been timely paid, the finality of the previous Office action has been withdrawn pursuant to

37 CFR 1.114. Applicant's submission filed on 21 December 2007 has been entered.

2.      Claims 1-20 have been presented for examination.

### Response to Arguments

3.      Applicant's arguments regarding the 35 U.S.C. 112, 2nd paragraph rejection filed 21

December 2007 have been fully considered but they are not persuasive. In response to applicant's

argument that the features upon which applicant relies are recited in the specification and not

recited in the rejected claims. The Applicant is reminded that although the claims are interpreted

in light of the specification, limitations from the specification are not read into the claims. See *In*

*re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

4.      Applicant's arguments with respect to the prior art rejection of claims 1-20 have been

considered but are moot in view of the new grounds of rejection.

5.      See further rejections set forth below.

### Claim Rejections - 35 USC § 112

6.      The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

7.      Claims 3, 4, and 9 are rejected under 35 U.S.C. 112, second paragraph, as being

indefinite for failing to particularly point out and distinctly claim the subject matter which

applicant regards as the invention.   Regarding claims 3, 4, and 9, it is unclear which versions of

the Iub and Iur Specifications the Applicant is referring to and appears to be attempting to cover

future versions of the both specifications.

### Claim Rejections - 35 USC § 103

8.      The text of those sections of Title 35, U.S. Code not included in this action can be found

in a prior Office action.

9.      Claims 1, 5, 6, and 13-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over

U.S. Patent No. 6,996,712 to Perlman et al., hereinafter Perlman, in view of U.S. Patent

Application Publication No. 2005/0013324 A1 to Leahy et al., hereinafter Leahy.

10.     As per claim 1, Perlman teaches an apparatus, comprising:

        a network interface (Figures 2 and 4 [block 15]) to communicate frames of information in

accordance with a protocol (column 3, lines 57-60, i.e. the end station sends data packets to

recipients via network interface in a known manner); and

        a frame authentication module operatively responsive to said network interface (Figure 2

[block 14]), said frame authentication module to authenticate multiple frames communicated by

said network interface (column 4, lines 4-19, column 5, lines 49-52, i.e. authenticating the

received data packets, selecting bytes from each of the received data packets to perform the

integrity check), with each frame containing authentication information in a spare extension field

(Figure 3 [block 34], column 4, lines 64-66, column 7, lines 50-67, i.e. the integrity block is

included in the data packet) or encode multiple frames with authentication information if the

frames do not include authentication information (column 3, lines 51-60, column 4, lines 1-3, column 4, lines 64-66, column 5, lines 53-61, i.e. produce an encrypted integrity block for a single data packet, using an integrity check for each packet, implying that there are more than one packet and Perlman's use of the plural data packets).

11.    Perlman does not teach the use of a wireless protocol.

12.    Leahy teaches validating incoming packets based on a key included in the packet that is equally applicable to both wired and wireless networks regardless of the physical topology or protocols used (paragraph 0047).

13.    It would have been obvious to one of ordinary skill in the art at the time the invention was made to implement the packet authentication using a wireless protocol since Perlman discloses at column 3, line 60 that any known protocol may be used.  Furthermore networks are limited to either being wired or wireless, so it would have only required ordinary skill in the art could to try implementing the authentication scheme in either a wired or wireless environment. See *KSR International Co. v. Teleflex Inc.*, 82 USPQ2d 1385 (U.S. 2007).


14.    Regarding claims 5 and 10, Perlman teaches wherein said authentication module comprises:

an authentication encoding module to encode each frame with authentication information (column 3, lines 50-60, i.e. during a send, creating integrity checks); and

an authentication decoding module to authenticate each frame using said authentication information (column 4, lines 39-63, i.e. recipient decrypts the integrity blocks).

15.    With regards to claims 6 and 11, Perlman teaches wherein said authentication encoding

module generates said authentication information using an authentication key (i.e. shared secret

key), data from said frame (i.e. data bytes from one or more data packets), and a change

parameter (column 3, lines 4-25, i.e. selected information, timestamp, packet sequence numbers)

(column 3, lines 50-57).

16.    As per claims 13 and 17, Perlman teaches a method and an article, comprising:

    receiving multiple frames of information over a medium (column 4, lines 3-19, column 5,

lines 49-52, i.e. authenticating the received data packets, selecting bytes from each of the

received data packets to perform the integrity check);

    determining whether each frame includes authentication information (column 3, lines 60-

64, column 4, line 64 to column 5, line 3, i.e. the integrity block may be in a separate packet, the

authentication information does not have to be in transmitted packet, instead traveling

independently) in a spare extension field (Figure 3 [block 34], column 4, lines 64-66, column 7,

lines 50-67, i.e. the integrity block is included in the data packet);

    authenticating each frame using said authentication information (column 4, lines 3-9,

column 4, lines 40-63); and

    encoding each frame with authentication information if said frame does not include said

authentication information (column 3, lines 51-60, column 4, lines 1-3, column 6, lines 14-27).

17.    Perlman does not teach the use of a wireless protocol.

18.     Leahy teaches validating incoming packets based on a key included in the packet that is

equally applicable to both wired and wireless networks regardless of the physical topology or

protocols used (paragraph 0047).

19.     It would have been obvious to one of ordinary skill in the art at the time the invention

was made to implement the packet authentication using a wireless protocol since Perlman

discloses at column 3, line 60 that any known protocol may be used. Furthermore networks are

limited to either being wired or wireless, so it would have only required ordinary skill in the art

could to try implementing the authentication scheme in either a wired or wireless environment.

See *KSR International Co. v. Teleflex Inc.*, 82 USPQ2d 1385 (U.S. 2007).

20.     Regarding claims 14 and 18, Perlman teaches retrieving an authentication key (column 4,

lines 39-63, i.e. shared secret key);

        duplicating said authentication information using said authentication key (column 4, lines

41-63, i.e. reproducing the integrity checks);

        retrieving said authentication information from each frame (column 4, lines 39-63);

        comparing said duplicated authentication information with said retrieved

authentication information (column 4, lines 43-63); and

        authenticating each frame in accordance with said comparison (column 4, lines 43-63).

21.     Regarding claims 15 and 19, Perlman teaches generating said authentication information

(column 3, lines 50-58, i.e. generate integrity block); and

storing said authentication information in a spare extension field of each frame (Figure 3 [block 34], column 7, lines 50-67).

22.    With regards to claims 16 and 20, Perlman teaches retrieving an authentication key (column 3, lines 50-57, i.e. shared secret key);

retrieving data from each frame (column 3, lines 50-57, i.e. data bytes from one or more data packets);

retrieving a change parameter (column 3, lines 4-25, column 3, lines 50-57, i.e. selected information, timestamp, packet sequence numbers); and

creating said authentication information in accordance with an authentication algorithm using said authentication key, said data, and said change parameter (column 3, lines 50-57).

23.    Claim 2 is rejected under 35 U.S.C. 103(a) as being unpatentable over Perlman in view of Leahy as applied above, and in further view of **draft 3G TS 22.100**, hereinafter **TS 22.100**.

24.    Claim 8 is rejected under 35 U.S.C. 103(a) as being unpatentable over Perlman in view of **TS 25.427** as applied to claim 7 below, and further in view of **TS 22.100**.

25.    Regarding claims 2 and 8, Perlman does not teach wherein said network interface comprises a network interface defined in accordance with the Universal Mobile Telecommunication System.

26.    **TS 22.100** teaches wherein said network interface comprises a network interface operable with a Universal Mobile Telecommunication System (pages 7-9).

27.    It would have been obvious to one of ordinary skill in the art at the time the invention

was made for the network interface to comply with the UMTS specification, since **TS 22.100**

discloses a number of security features on page 12, which include, but are not limited to, mutual

authentication between the user and the serving network, confidentiality of user and signaling

data, and end-to-end encryption.

28.    Claims 3, 4, and 9-12 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Perlman in view of Leahy as applied above, and in further view of **3G TS 25.427**, hereinafter **TS**

**25.427.**

29.    Regarding claims 3 and 9, Perlman does not disclose wherein said network interface

comprises a network interface configured in accordance with one of an Iub Specification and an

Iur Specification.

30.    **TS 25.427** teaches wherein said network interface comprises a network interface

configured in accordance with one of an Iub Specification and an Iur Specification (Figures 1

and 2, page 7-80).

31.    It would have been obvious to one of ordinary skill in the art at the time the invention

was made for the network interface to be configured in accordance with the Iub and Iur

specifications, **TS 25.427** states at page 7 that all the set of cells are carried on one transport

connection, which means there are as many transport connects as set of coordinated transport

channels and user ports for that communication, thereby preventing any traffic bottlenecks.

32. Regarding claim 4, Perlman does not teach wherein said wireless protocol comprises a framing protocol defined by one of an Iub Specification and an Iur Specification.

33. **TS 25.427** teaches wherein said wireless protocol comprises a framing protocol defined by one of an Iub Specification and an Iur Specification (pages 11-21).

34. It would have been obvious to one of ordinary skill in the art at the time the invention was made to format the data packets in accordance with the framing protocol disclosed in the Iub and Iur specifications, since **TS 25.427** states on page 12 that the purpose of the user data frames is to transparently transport the data blocks between the node and the radio network controller.

35. Claim 7 is rejected under 35 U.S.C. 103(a) as being unpatentable over Perlman in further view of **3G TS 25.427**, hereinafter **TS 25.427**.

36. As per claim 7, **TS 25.427** teaches a system, comprising:

a node B system having a first network interface (page 8, Figures 1 and 2, i.e. NB sending and receiving data from SNRC);

a first radio network controller to communicate with said node B system, said first radio network controller having a second network interface (page 8, Figures 1 and 2, i.e. SRNC sending and receiving data from NB).

37. **TS 25.427** does not teach a frame authentication module for each of said first and second network interfaces, said frame authentication module to authenticate frames communicated between said first and second interfaces.

38. Perlman teaches a frame authentication module for each of said first and second network interfaces (Figure 2 [block 14], column 3, line 50, i.e. each end station includes an authentication

system), said frame authentication module to authenticate multiple frames communicated

between said first and second interfaces (column 4, lines 1-19, column 4, lines 39-63, column 5,

lines 49-52, i.e. authenticating the received data packets, selecting bytes from each of the

received data packets to perform the integrity check), with each frame containing authentication

information in a spare extension field (Figure 3 [block 34], column 4, lines 64-66, column 7,

lines 50-67, i.e. the integrity block is included in the data packet) or encode multiple frames with

authentication information if the frames do not include authentication information (column 3,

lines 51-60, column 4, lines 1-3, column 4, lines 64-66, column 5, lines 53-61, i.e. produce an

encrypted integrity block for a single data packet, using an integrity check for each packet,

implying that there are more than one packet and Perlman's use of the plural data packets).

39.     It would have been obvious to one of ordinary skill in the art at the time the invention

was made to implement the authentication system of Perlman on the systems of Node B and

radio network controller, since Perlman states at column 2, lines 2-10 that the authentication

system would be fast and uncomplicated and would add robustness to the systems.


40.     Regarding claim 12, Perlman and **TS 25.427** do not teach a second radio network

controller to communicate with said first radio network controller, said second radio network

controller having a third network interface; and a frame authentication module for said third

network interface, said frame authentication module to authenticate frames communicated

between said second and third interfaces.

41.     It would have been obvious to one of ordinary skill in the art at the time the invention

was made to include a second radio network controller having a third interface with its own

frame authentication module, since it has been held that it only requires routine skill in the art to merely duplicate a part, in this case the second radio network controller. See MPEP § 2144.04; see also *In re Harza*, 274 F.2d 669, 124 USPQ 378 (CCPA 1960).

*Conclusion*

42.    Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian La Forgia whose telephone number is (571) 272-3792. The examiner can normally be reached on Monday thru Thursday 7-5.

43.    If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

44.    Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Christian LaForgia
Patent Examiner
Art Unit 2131

clf